

Windows Azure Network Security

Author: Ashwin Palekar, Principal Program Manager, Windows Azure

Published: November 2013  
Microsoft Corporation

**Contributors**

**Narayan Annamalai, Senior Program Manager, Windows Azure**

**Gareth Bradshaw, Senior Program Manager, Windows Azure**

**Jeff Gollnick, Senior Content Publishing Manager, CE CSI**

**Charlie Kaufman, Principal Program Manager, Windows Azure**

**Yousef Khalidi, Distinguished Engineer, Windows Azure**

**Cheryl McGuire, Technical Writer, CE CSI**

**Parag Sharma, Principal Software Development Engineer, Windows Azure**

**Joel Sloss, Consultant, Windows Azure**

**Kamal Srinivasan, Program Manager, Windows Azure**

**Reviewers**

**Deepak Bansal, Principal Development Manager**

**Ramesh Chinta, Principal Group Program Manager, Windows Azure**

**Daniel Firestone, Software Development Engineer, Windows Azure**

**Karthick Jayaraman, Software Development Engineer, Windows Azure**

**Dave Maltz, Partner Development Manager, Windows Azure**

**Geoff Outhred, Principal Software Development Engineer Lead, Windows Azure**

**NK Srinivas, Principal Program Manager Lead, Windows Azure**

**Mark Russinovich, Technical Fellow, Windows Azure**

**Copyright Information**

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Microsoft, SQL Server, Windows PowerShell, Windows, Windows Azure, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

© 2013 Microsoft Corporation. All rights reserved.

Contents

[Abstract 4](#_Toc373323668)

[Introduction 4](#_Toc373323669)

[Guidelines for Securing Infrastructure as a Service 4](#_Toc373323670)

[Security Management and Threat Defense 10](#_Toc373323671)

[Guidelines for Securing Platform as a Service 12](#_Toc373323672)

[Appendix: Windows Azure Network Security Internals 13](#_Toc373323673)

[Isolation 13](#_Toc373323674)

[Microsoft Services 13](#_Toc373323675)

[References 14](#_Toc373323676)

# Abstract

This document provides guidance on securing network communication for applications deployed in Windows Azure, enabling customers to determine how best to protect their virtual infrastructure and data.

The intended audience for this whitepaper includes:

* IT and Network administrators interested in deploying applications on Windows Azure
* Developers interested in creating applications that run on Windows Azure
* Technical decision makers (TDMs) considering Windows Azure to support new or existing services

# Introduction

To build and manage solutions in the cloud that comply with industry standards and regulations, IT administrators should understand the security mechanisms within Windows Azure—both those that are automatic and those that require configuration.

In particular, Windows Azure networking provides the infrastructure necessary to securely connect your virtual machines to one another, as well as bridge between the cloud and your on-premises datacenter.

The overall architecture and operation of Windows Azure’s network services have been designed for flexibility, security, and integrity. This white paper seeks to uncover these inner-workings and give insights on how customers can take advantage of the platform’s native features to best protect their information assets.

# Guidelines for Securing Infrastructure as a Service

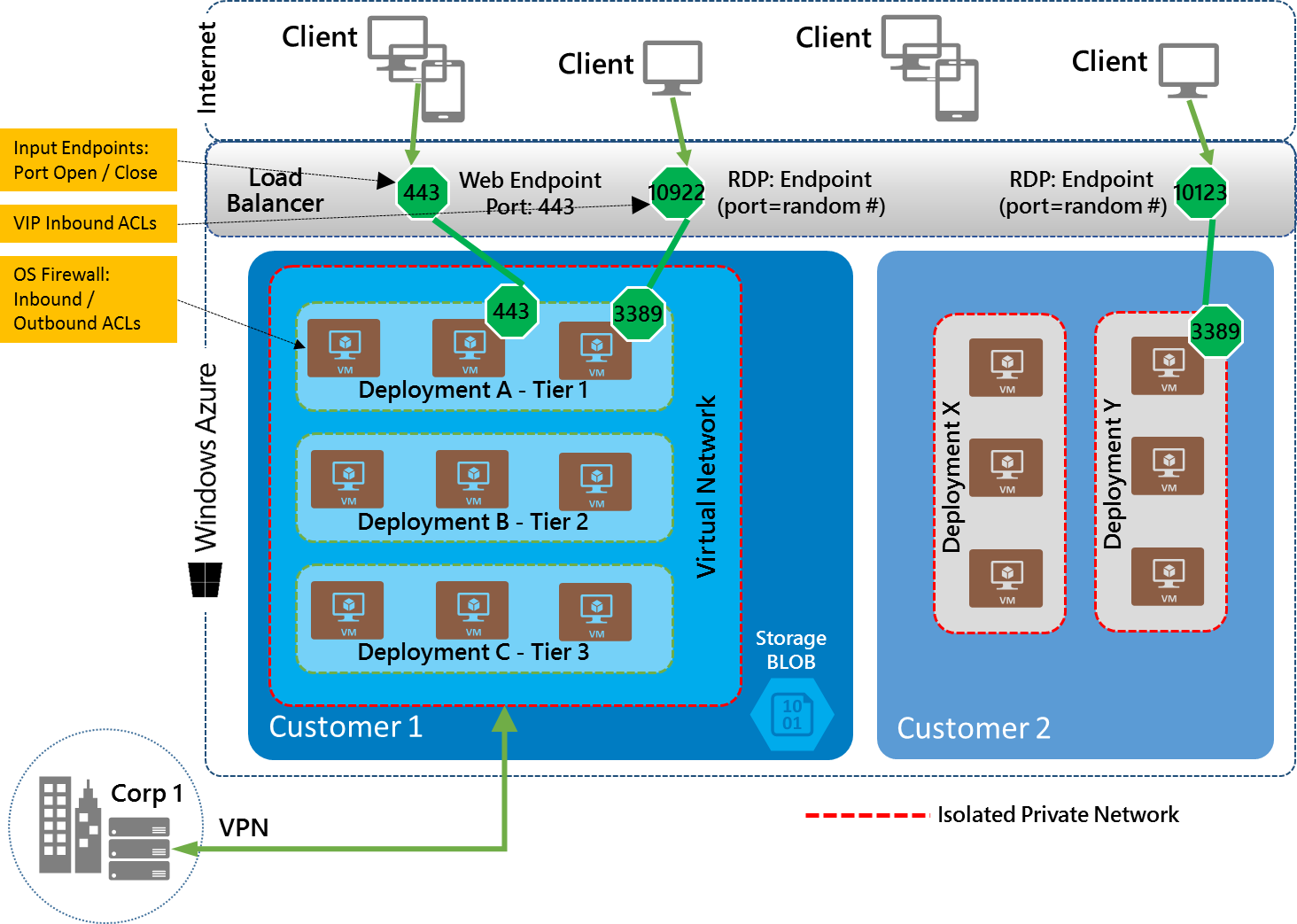
Cloud vendors that offer Infrastructure as a Service (IaaS) provide the shared hardware and software systems for multiple simultaneous customer deployments, running numerous workloads and configurations. Customers who subscribe to IaaS typically have their own operating systems and applications which will run on this infrastructure inside virtual machines (VMs), relying on the core security capabilities delivered by the vendor. This differs from the traditional datacenter model where a company’s IT organization retains ultimate control over networked systems, including physical access to networking equipment—in the cloud, the responsibility is shared between the vendor and the customer.

Fundamental to any shared cloud architecture is the isolation provided for each customer. In Windows Azure, a customer subscription can include multiple deployments, and each deployment can contain multiple VMs. Windows Azure provides network isolation at several points:

* Deployment: Each deployment is isolated from other deployments. Multiple VMs within a deployment are allowed to communicate with each other through private IP addresses.
* Virtual Network: Multiple deployments (inside the same subscription) can be assigned to the same virtual network, and then allowed to communicate with each other through private IP addresses. Each virtual network is isolated from other virtual networks.

An example of such a topology is shown in Figure 1.

Virtual machines do not receive inbound traffic from the Internet, except through a set of customer-defined input endpoints. An input endpoint defines which VM:port mapping should receive inbound traffic coming from outside a deployment’s isolated network—this means traffic could come from the Internet as well as from other VMs inside Windows Azure.



**Figure 1. An example of isolated multi-tier IaaS applications hosted within Windows Azure.**

Following are the principal network security considerations for administrators when deploying or migrating virtual machines in Windows Azure.

|  |  |  |
| --- | --- | --- |
| Securing communications between VMs |  | Virtual machines inside a deployment are allowed to communicate with each other via private IP addresses. Communication between VMs in multiple deployments of a subscription can be secured by using virtual networks.  In addition to virtual networks, for enhanced security (similar to on-premises networks), it is possible to use IPsec-based security for all communications. |
| Securing inbound communications from the Internet |  | By default, every VM created through the Windows Azure Management Portal has inbound traffic flow blocked from the Internet, except for remote management ports.  By configuring input endpoints, administrators decide which VM ports can be accessed from the Internet. Below are some common configuration changes to more securely control remote access at a network level from the Internet to ports on VMs.  IT administrators can restrict access by:   * Defining input endpoints to only open ports that you need. * Specifying IP access control lists (ACLs) on input endpoints, to control the source IPs from which the VM will allow traffic. * Only allowing connectivity from your on-premises corporate network using a site-to-site VPN. Add the VMs to a virtual network, and connect the virtual network to your corporate network via a virtual network gateway. * Using a proxy firewall (such as the Web Application Firewall or NG Firewall virtual appliances from Barracuda Networks) that runs on a virtual machine to filter traffic to the VM. Add the VMs to a virtual network, and then define an input endpoint that points to a port on the proxy firewall. * Only opening ports you need inside the firewall in the guest OS.   If an application exposes input endpoints, it should follow the same security model as if it were running open on the Internet. If the application sends or receives any sensitive data on the input endpoints, then all input endpoints should use server and client authentication, and communication should be encrypted. |
| Securing communications across subscriptions |  | A customer may have multiple subscriptions, and VMs may need to communicate between multiple subscriptions. For this case, VMs can be configured to communicate via public virtual IP addresses, and IP ACLs on input endpoints can be used to allow those VMs to initiate connections only with each other. However, creating ACLs based on IP addresses is not ideal, since the ACLs must be updated any time the public virtual addresses change. This can result in service failures and puts additional burden on the administrator. Public virtual IP addresses can change after compute resources are de-allocated when a virtual machine is shut down, or after a deployment is deleted. Using in-place upgrade enables administrators to deploy new versions of their service without the Public IPs of the VMs changing.     * For more information on configuring IP ACLs, see [About Network Access Control Lists](http://go.microsoft.com/fwlink/p/?linkid=303816&clcid=0x409) |
| Securing communications across regions |  | If an application sends or receives any sensitive data across Windows Azure regions, then communications must be encrypted. Cross-region traffic transits over a WAN and is more open to interception.  Within Windows Azure regions, customers with security concerns should use encryption for all communication that leaves a VM. For example, regulatory compliance standards may require this extra security measure. |
| Securing communications to on-premises networks |  | When customers’ workloads require secure communications between the Windows Azure Virtual Network and their on-premises systems, it is best to protect those channels using a virtual network gateway.  There are two typical scenarios:   1. Internal Multi-tier Application: A multi-tier application is deployed on Windows Azure, and the application does not need any inbound connectivity from the Internet. However, the application needs connectivity to servers and applications in the customer’s corporate network, as shown in Figure 2.     **Figure 2. VPN between a corporate network and Windows Azure.**  In this case, you can create a virtual network and add the VMs of the application tiers to the virtual network, but you do not define any input endpoints. Remove the remote management input endpoints or lock them down using the guidance provided below to secure management endpoints. Then, configure the virtual network gateway so that traffic destined for the corporate network flows through the VPN to the target servers / network devices.   1. Public-facing Multi-tier Application: A multi-tier application is deployed in Windows Azure, and the front-end tier requires inbound connectivity from the internet. The back-end tiers do not need inbound connecitivty from the internet, but do need connectivity to the customer’s corporate network.     **Figure 3. Addition of Internet-facing endpoints.**  In this case, you can create a virtual network with the appropriate VMs from each of the application tiers, define input endpoints for VMs in the front-end tier, and then remove the remote management input endpoints or lock them down. Configure the virtual network gateway so that traffic destined to the corporate network flows through the VPN and to the corporate network.  The virtual network gateway establishes an IPsec tunnel between the virtual network and the customer’s VPN device (which can be either a hardware VPN device or a software VPN such as Windows Server 2012 Routing and Remote Access Services), and routes traffic appropriately.  Creating a virtual private network within Windows Azure provides the ability to more securely extend your on-premises network into Windows Azure. This connection can either be site-to-site or point-to-site.  For more information on virtual network gateway configuration, see [Configure a Virtual Network Gateway in the Management Portal](http://msdn.microsoft.com/en-us/library/windowsazure/jj156210.aspx). |
|  |  |  |

## Security Management and Threat Defense

|  |  |  |
| --- | --- | --- |
| Securing remote management of VMs |  | By default, if a VM is created through the Windows Azure Management Portal, RDP and Powershell ports are opened. When a VM is created through Powershell, RDP and Powershell ports must be explicitly opened. The Portal assigns RDP and Powershell port numbers using a random number to reduce the chances of a password dictionary attack. You can choose to keep the RDP and Powershell ports open to the Internet, but at a bare minimum, secure the VMs with strong passwords. In addition, consider using the general options to secure inbound communication from the Internet mentioned above. |
| Protecting against DDOS |  | Windows Azure has a distributed denial-of-service (DDoS) defense system that helps prevent attacks against Windows Azure platform services. It uses standard detection and mitigation techniques such as SYN cookies, rate limiting, and connection limits.  Windows Azure’s DDoS defense system is designed not only to withstand attacks from the outside, but also from within.   * For attacks launched from the outside (Internet), IP addresses can be spoofed, although they are prevented from spoofing Windows Azure datacenter IP address ranges. * For attacks launched from within a tenant, trusted packet filters prevent impersonation (spoofing) of Windows Azure IP addresses inside the Windows Azure datacenter. * Windows Azure monitors and detects internally initiated DDoS attacks and removes offending VMs from the network.   Windows Azure’s DDoS protection also benefits applications. However, it is still possible for applications to be targeted individually. As a result, customers should actively monitor their Windows Azure applications. For more information, see [Collect Logging Data by Using Windows Azure Diagnostics](http://msdn.microsoft.com/en-us/library/gg433048.aspx).   * Proxy devices (such as web application firewalls) that terminate and then forward traffic to endpoints can run in a virtual machine, and provide protection against an even broader range of DoS and other attacks (e.g. low-rate, HTTP, and application-layer threats). * Some virtualized solutions available are also capable of both intrusion detection and prevention. * You can also deploy more instances of your application to handle the potentially higher load generated by an attack. For more information on these techniques, see [Disaster Recovery and High Availability for Windows Azure Applications](http://msdn.microsoft.com/en-us/library/windowsazure/dn251004.aspx).   If a customer notices their application is under attack, they should contact Windows Azure [Customer Support](http://www.windowsazure.com/en-us/support/contact/) to receive assistance. Windows Azure Customer Support personnel are trained to react promptly to these types of requests. |
| Intrustion detection and prevention |  | Certain appliances such as Web Application Firewalls (WAF) can proxy communications by terminating and then forwarding the traffic to endpoints, also applying intrusion detection and prevention, as well as denial of service mitigation techniques. Virtual appliance form-factors should work on Windows Azure as long as they are certified by the vendor to do so. |
| Securing internal VM names with internal DNS |  | To allow VMs within a cloud service to be addressed by name, Windows Azure provides an internal DNS service. VM names are resolved to private IP addresses within a cloud service while maintaining privacy across cloud services, even within the same subscription.  The private IP addresses assigned to both Cloud Service roles and Virtual Machines can change during repair. Due to this, communication between roles within a Windows Azure hosted service must be resolved via DNS name and not by IP address. The one exception to this rule is when virtual networks are being used for custom IP address spaces. In those cases, IP addresses can be assumed to be static. Also, as private IP addresses can change, the DNS TTL (time-to-live) values of the DNS responses should be honored in the client. |
| Securing communication from VM to Windows Azure SQL Database |  | Windows Azure SQL Database also provides a built-in firewall to filter incoming traffic. Initially, all communication with the SQL database is blocked. To enable communication with the database, firewall rules must be defined in Windows Azure SQL Database allowing the public IP address of the VM in Windows Azure to communicate with the data source.  However, creating ACLs based on IP addresses is not ideal, since the ACLs must be updated any time the public virtual addresses change. This can result in service failures, and puts additional burden on the administrator. Public virtual IP addresses can change after compute resources are de-allocated when a virtual machine is shut down, or after a deployment is deleted. Using in-place upgrade enables administrators to deploy new versions of their service without the public IPs of the VMs changing.     * For more information on how to configure IP ACLs, see [About Network Access Control Lists](http://go.microsoft.com/fwlink/p/?linkid=303816&clcid=0x409)   To learn about configuring the SQL Database firewall to specify rules at both the server-level and database-level, refer to the following articles:   * [Windows Azure SQL Database Firewall](http://msdn.microsoft.com/en-us/library/windowsazure/ee621782.aspx) * [sp\_set\_firewall\_rule (Windows Azure SQL Database)](http://msdn.microsoft.com/en-us/library/windowsazure/ff951635.aspx) |

# Guidelines for Securing Platform as a Service

The above guidelines for IaaS also apply to Web roles and Worker roles (PaaS roles). However, IP ACLs on Virtual IPs (VIPs) are not supported for the Web/Worker Role.

As with IaaS VMs, every PaaS role created through the Windows Azure Portal has inbound traffic flow blocked from the Internet by default, including remote management ports. When a PaaS role is enabled for remote desktop, the RDP port is opened. RDP port numbers are assigned using a random number to reduce the chances of a broad scanning/password dictionary attack.

Customers can choose to keep the RDP ports open to the Internet, but at a bare minimum should secure the PaaS role with a strong password. When using RDP, enable the RDP port through the Windows Azure Portal, but then disable the port after using it.

Similarly, only open other ports by defining them in the Endpoints element of the WebRole or WorkerRole schema in the service definition file (.csdef). For more information, see [WebRole Schema](http://msdn.microsoft.com/en-us/library/windowsazure/gg557553.aspx) and [WorkerRole Schema](http://msdn.microsoft.com/en-us/library/windowsazure/gg557552.aspx).

# Appendix: Windows Azure Network Security Internals

This section provides additional depth regarding internals of Windows Azure network security, as well as some guidelines for securing services built on of Windows Azure.

## Isolation

Windows Azure provides network isolation for each deployment with multiple enforcement points. Using input endpoints, customers decide which ports can be accessed from the Internet.

1. Traffic between VMs always traverses through trusted packet filters. VMs cannot send or receive any Layer-2 traffic. Thus, a VM cannot snoop any traffic on the network that is not destined to it. ARP requests from a VM are rate-limited and cannot be spoofed. In addition, a VM cannot send ARP responses on behalf of other VMs or hosts in the same subnet. The VM cannot send any DHCP responses and can send only DHCP requests (capped at fixed rate). Only the Network Manager, which is a component of Windows Azure’s infrastructure, is allowed to send DHCP responses.
2. Azure infrastructure is protected from customer VMs at multiple layers. There are mechanisms in place to ensure that customer VMs cannot send traffic to key Azure infrastructure VMs- Customer VMs can only talk to the Azure infrastructure endpoints that are meant for public communication. In addition, all Windows Azure infrastructure endpoints are secured via HTTPS.
3. Customers can put their VMs in a deployment, and can also choose to put deployments into a virtual network (VNET). In both cases, VMs get their own address spaces that are completely invisible, and hence, not reachable from VMs outside of a deployment or VNET (unless configured to be visible via public IP addresses).
4. VMs can only be accessed from the Internet on ports (input endpoints) that the application has declared for public access. Windows Azure programs the infrastructure to open only the ports specified by the customer for public access.

## Microsoft Services

This section lists some of the guidance provided to secure communication for Microsoft services that run on of Windows Azure.

* Services must follow the same model as if they were running in the open Internet, whether or not the service and its clients are running within Windows Azure. This implies that all exported endpoints that transmit sensitive data should use SSL/TLS (HTTPS).
* Internet facing endpoints of all Microsoft services must be SSL/TLS protected by default. This helps mitigate the risk of network-based sniffing or tampering with customer data, administrative and portal functions, as well as countless other data flows. Client-side interfaces provided by Azure and exposed to developers must be built to use SSL/TLS by default, and should not fall back to attempting non-SSL connections.
* Applications can rely on Azure to protect their intra-deployment traffic. In addition, applications can rely on Azure to protect their intra-VNET traffic as long as they use internal endpoints that are not accessible from outside the VNET. Deployments and VNETs are contained within Azure regions and therefore their traffic does not span regions. SSL can be used for intra-deployment/VNET traffic as an extra security measure.
* Inter-Deployment traffic that uses Internet facing endpoints must be treated as Internet facing traffic that is SSL/TLS protected by default.
* Traffic across Windows Azure regions must be treated the same as the traffic that is crossing the open Internet and therefore must use SSL/TLS.

# References

MSDN documentation on Windows Azure Network Service <http://msdn.microsoft.com/en-us/library/windowsazure/gg433091.aspx>